

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-272561

(43)Date of publication of application : 08.10.1999

---

(51)Int.Cl. G06F 12/14  
G06F 3/06

---

(21)Application number : 10-068881 (71)Applicant : FUJITSU LTD  
(22)Date of filing : 18.03.1998 (72)Inventor : KOBAYASHI HIROYUKI  
UCHIDA YOSHIAKI

---

(54) DATA PROTECTION METHOD FOR STORAGE MEDIUM DEVICE FOR THE SAME AND  
STORAGE MEDIUM THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To change key data for each storage unit by one word in a data protection method for a storage medium and its device which encipher data to be recorded in the storage medium by a password and perform protection of the data.

SOLUTION: This device has a step which has a password PW encipher 20 key data P5 and writes them in a storage medium 1 after generating the key data P5 and a step which has the key data encipher 21 data and write them in the storage medium 1. Moreover it has a step which reads the enciphered key data from the storage medium 1 a step which has the password decode 22 the enciphered key data and a step which has the decoded key data decode 23 the data of the storage medium 1. Since enciphering is performed by using the key data generated separately from the password an analysis of the password by decoding of a cryptogram is prevented.

---

## CLAIMS

---

[Claim(s)]

[Claim 1] In a data protection method of a storage for protecting data of a storage Generate key data and said key data is enciphered with a password Data is enciphered as a step written in said storage with said key data A step written in said storage and a step which reads said enciphered key data from

said storageA data protection method of a storage having a step which decrypts said enciphered key data with said passwordand a step which decrypts data of said storage by said decrypted key data.

[Claim 2]A data protection method of a storagewherein a step which generates said key data in a data protection method of a storage of Claim 1 is a step which generates said key data for every logical sector of said storage.

[Claim 3]A data protection method of a storagewherein a step which generates said key data in a data protection method of a storage of Claim 2 is a step which generates said key data for said every logical sector at the time of writing of said data.

[Claim 4]A data protection method of a storagewherein a step which generates said key data in a data protection method of a storage of Claim 1 is a step which generates said key data combining a number of random data defined beforehand.

[Claim 5]A data protection method of a storage of Claim 1 characterized by comprising the following.

A step decrypted with an old password specified by a user after reading said enciphered key data from said storage.

A step which writes in key data enciphered to said storage after enciphering said decrypted key data with a new password specified by a user.

[Claim 6]In a data protection method of a storage of Claim 1a step which writes said enciphered key data in said storageAre a step which enciphers said key data and writes said enciphered each key data in said storage in each of two or more passwordsand a step which decrypts said key dataA data protection method of a storage being a step decrypted with a password which had said read key data which was enciphered specified.

[Claim 7]In a data protection method of a storage of Claim 1a step which writes said enciphered key data in said storageWith a password of lencipher said key dataand write said enciphered key data in said storageand other passwords are enciphered with a password of lAre a step which writes in other enciphered passwords and a step which decrypts said key dataA data protection method of a storage being a step which decrypts said password of enciphered others with a password besides the aboveand obtains said password of l and a step which decrypts said enciphered key data with said password of l.

[Claim 8]A data protection device of a storage for protecting data of a storage characterized by comprising the following.

A storage.

A write mode which enciphers said key data with a passwordis written in said storageand enciphers data with said key data and is written in said storage after it has a lead and a control circuit which carries out a light for data

of said storage and said control circuit generates key data.

A Read mode which decrypts said enciphered key data with said password and decrypts data of said storage by said decrypted key data after reading said enciphered key data from said storage.

[Claim 9] A data protection device of a storage wherein said storage comprises a storage by which read/write is carried out for every logical sector in a data protection device of a storage of Claim 8 and said control circuit generates said key data for every logical sector of said storage.

[Claim 10] A data protection device of a storage wherein said control circuit generates said key data for said every logical sector in a data protection device of a storage of Claim 9 at the time of writing of said data.

[Claim 11] A data protection device of a storage wherein said control circuit generates said key data in a data protection device of a storage of Claim 8 combining a number of random data defined beforehand.

[Claim 12] In a data protection device of a storage of Claim 8 said control circuit After reading said enciphered key data from said storage it decrypts with an old password specified by a user And a data protection device of a storage characterized by writing in key data enciphered to said storage after enciphering said decrypted key data with a new password specified by a user.

[Claim 13] A data protection device of a storage of Claim 8 characterized by comprising the following.

A write mode which said control circuit enciphers said key data in each of two or more passwords and writes said enciphered each key data in said storage.

A Read mode decrypted with a password which had said read key data which was enciphered specified.

[Claim 14] A data protection device of a storage of Claim 8 characterized by comprising the following.

A write mode which writes in other passwords which said control circuit is a password of 1 and enciphered said key data wrote said enciphered key data in said storage and enciphered other passwords with a password of 1 and were enciphered.

A Read mode which decrypts said enciphered key data with said password of 1 after decrypting said password of enciphered others with a password besides the above and obtaining said password of 1.

[Claim 15] A storage which has the protected data comprising:

Key data enciphered with a password.

Data enciphered with said key data.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] In an information management system this invention enciphers with a password the data recorded on a storage and relates to the data protection method of the storage for protecting data its device and its storage.

[0002] The memory storage using an optical disc a magnetic disk an IC card etc. is used for various information management systems such as a computer a word processor and an Electronic Book. In this memory storage information including information extra sensitive information in the course of duties etc. concerning privacy not to be known originally in addition to an owner may be written in. In order that others may not know such information it is necessary to encipher data.

[0003]

[Description of the Prior Art] Drawing 15 is an explanatory view of conventional technology.

[0004] A password is set up to the storage 90 or memory storage such as an optical disc. When writing in data data is enciphered with a password by the encryption section 91 and it writes in the storage 90. At the time of read-out the data of the storage 90 is decrypted with a password by the decoding section 92.

[0005] Thus data can be kept secret by enciphering data. In this case there was a method which sets one password as the whole storage conventionally. There is also a method which sets up a password which is different in the file basis of a storage.

[0006]

[Problem(s) to be Solved by the Invention] However there was the following problem in conventional technology.

[0007] A decoder's decipherment becomes easy so that there is much combination of the plaintext which is not enciphered [ 1st ] as the cryptogram or cryptogram as a sample. Since the result of having enciphered the same plaintext with the same password is equal when it enciphers directly with the same password the statistical property of a cryptogram reflects the statistical property of a plaintext. Therefore in the method which enciphers the conventional storage with the same password when it was in the large quantity so that the statistical work of the cryptogram could be carried out there was a

problem that the character of a plaintext could be presumed easily.

[0008]There is a portion which comprises fixed form formatssuch as the directory portionin the data saved [ 2nd ] at mass storage mediasuch as an optical disc. In the method which enciphers the conventional storage with the same passwordwhen the password was presumed by analyzing such a portionthere was a problem that other important data will be decoded.

[0009]In the method which sets a password as the 3rd for every conventional filethe decipherment of other portions can be prevented by the decipherment of some passwords. Howeverit is necessary to manage a password which is different for every file in this case. For this reasonthere was a problem of it having been complicated and being easy to cause accidentssuch as password oblivion.

[0010]In exchangeable mass storage mediasuch as an optical discit is [ 4th ] possible to carry out a storage or to copy a storage. For this reasonit is possible to carry out the once enciphered data and to analyze slowly.

Thereforethere was also a problem of being easy to presume a password from a cryptogram.

[0011]Since it had enciphered [ 5th ] directly with the password conventionallywhen the password was changedthere was also a problem that it was necessary to re-encipher the whole data.

[0012]The purpose of this invention is to provide the data protection method of a storage that a password is hard to be analyzed from a cryptogramits deviceand its storage.

[0013]Other purposes of this invention are one passwordand there are in providing the data protection method of a storage that key data is changeable into each storage unitits deviceand its storage.

[0014]Even if the purpose of further others of this invention changes a passwordthere is in providing the data protection method of the storage which makes re-encryption of data unnecessaryits deviceand its storage.

[0015]

[Means for Solving the Problem]After a data protection method of a storage of this invention generates key datait enciphers said key data with a passwordand has a write mode which has a step written in said storageand a step which enciphers data with key data and is written in said storage. And a step to which the data protection method reads said enciphered key data from a storageIt has a Read mode which has a step which decrypts enciphered key data with said passwordand a step which decrypts data of said storage by decrypted key data.

[0016]In this inventiondata is enciphered as a password using key data generated independentlynot using a password as a cryptographic key as it is. Key data enciphers a password as a key and writes it in a storage. At the time of read-outwith a passwordenciphered key data is decrypted and key data is

obtained. And data is decrypted by key data.

[0017]Thuseven if it analyzes a cryptogram by enciphering data as a password using key data generated independentlyenciphered key data is only decoded. For this reasonit is hard to analyze a password and key data. Therebya decipherment of a password in analysis of a cryptogram can be prevented.

[0018]A key which is different from a password in storage unitssuch as a sectorby changing key data to one password in order to encipher using key data generated independently can be given. For this reasonusing a different key for every logical sectorit can encipher and the confidentiality of data can be improved.

[0019]In order to encipher it as a password using key data generated independentlyeven if it changes a passwordre-encryption of data becomes unnecessary. For this reasoneven hundreds of megabytes of mass storage medium can realize change of a password easily.

[0020]

[Embodiment of the Invention]Drawing 1 the block diagram of the 1 embodiment of this invention and drawing 2The process flow figure at the time of the logical format of a 1st embodiment of this invention and drawing 3As for the writing processing flow chart of a 1st embodiment of this inventionand drawing 4the explanatory view of the key data of a 1st embodiment of this invention and drawing 6 of the explanatory view of the storage area of a 1st embodiment of this invention and drawing 5 are the reading processing flow charts of a 1st embodiment of this invention.

[0021]As shown in drawing 1the storage 1 comprises a magneto-optical disc. The logic sector size of this storage 1 shall be 2 KB (K byte). The control circuit 2 comprises a processor. The 1st encryption section 20 enciphers key data PS with the password PW which the user enteredand writes enciphered key data PS' in the storage 1.

[0022]The 2nd encryption section 21 enciphers the data which should be written in by key data PSand writes the enciphered data in the storage 1. The 1st decoding section 22 is decrypted with the password PW into which the user inputted key data PS' as which the storage 1 was enciphered. By decrypted key data PSthe 2nd decoding section 23 decrypts the data of the storage 1and outputs data. The memory 3 gives the work area of the control circuit (henceforth CPU) 2. The 1st and 2nd encryption section 20 and 21 and the 1st and 2nd decoding section 22 and 23 carry out processing of CPU2 to a blockand are shown.

[0023]Drawing 2 explains the processing at the time of logical format creation of a medium. The following processings are performed at the time of logical format creation of the medium which is the initial processing of a medium.

[0024] (S1) A user enters the user password PW into CPU2.

[0025] (S2) CPU2 generates the random number for a sector number (8 bytes). This random number is key data PS. Hereafter a sector number is set to n and it is PS. [1]- PS It explains as what generated the random number of [n].

[0026] (S3) CPU2 is random number (random data) PS for this sector number. [] (PS[1]- PS [n]) It stores in the work area of the memory 3.

[0027] (S4) CPU2 is key data PS of a work area. [1]- PS Each of [n] is enciphered with the password PW. Of course key data PS of a work area [1]- PS The whole [n] may be enciphered with the password PW.

[0028] (S5) Key data PS' as which CPU2 was enciphered [1]-PS' [n] is written in the field L1 of the storage 1.

[0029] As shown in drawing 4 the logical format of the storage (disk) 1 is shown by each sector. The address of this sector is carried out by logic block-address LBA. Hereby a diagram the sector of X individual is provided for LBA from "1" to "X."

[0030] Key data PS' enciphered in the field L1 for a sector from the heading sector (LBA=1) among the storage areas of this optical disc [1]-PS' It assigns the storing region of [n]. Namely key data PS' which the sector number of the use region of data is n (= (X-a)) and was enciphered by the field L1 for every sector of each use region [1]-PS' [n] is stored.

[0031] Next drawing 3 explains the writing processing of a medium.

[0032] (S10) Logic block-address (sector number) LBA presupposes that the write request to the position of "S0" arose. In order to keep the position which carries out a write request from lapping with the field L1 demanded sector number LBA is changed into "S1." Hereas shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0033] (S11) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc 1 and it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S14.

[0034] (S12) If the data of the field L1 reads CPU2 and it is not settled it will perform processing which develops key data to the work area of the memory 3. That is CPU2 obtains the user password PW. And data PS' of the field L1 of the optical disc 1 [1]-PS' [n] is read.

[0035] (S13) CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted with the password PW. Thereby it is key data PS. [1]- PS [n] is obtained. This key data PS [] (PS[1]- PS [n]) It stores in the work area of the memory 3.

[0036] (S14) CPU2 is key data PS of the key data of the work area of the memory 3 to logic block-address (sector number) LBA (=S0). [S0] is obtained. Key data PS corresponding to [ as shown in drawing 5 ] logic block-address LBA from the key data table of the work area of the memory 3 [S0] is obtained. And CPU2 is

this key data PS about the data which should be written in. It enciphers by [S0]. Well-known DES etc. can be used as the method of encryption.

[0037] (S15) CPU2 writes this enciphered data in the position of logic block-address LBA (=S1) of the optical disc 1.

[0038] Next reading processing is explained using drawing 6.

[0039] (S20) Logic block-address (sector number) LBA presupposes that the read request to the position of "S0" arose. In order to keep the position which carries out a read request from lapping with the field L1 demanded sector number LBA is changed into "S1." Hereas shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0040] (S21) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc 1 and it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S24.

[0041] (S22) If the data of the field L1 reads CPU2 and it is not settled it will perform processing which develops key data to the work area of the memory 3. That is CPU2 obtains the user password PW. And data PS' of the field L1 of the optical disc 1 [1]-PS' [n] is read.

[0042] (S23) CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted with the password PW. Thereby it is key data PS. [1]-PS [n] is obtained. This key data PS [] (PS[1]-PS [n]) It stores in the work area of the memory 3.

[0043] (S24) CPU2 is key data PS of the key data of the work area of the memory 3 to logic block-address (sector number) LBA (=S0). [S0] is obtained. Key data PS corresponding to [ as shown in drawing 5 ] logic block-address LBA from the key data table of the work area of the memory 3 [S0] is obtained. And CPU2 reads the data of the logic block address S1 from the optical disc 1. CPU2 is key data PS about the read data. It decrypts by [S0]. Well-known DES etc. can be used as the method of decryption. The decrypted data is sent out to a requiring agency (for example computer).

[0044] Thus at the time of logical format creation of a medium for every logical sector a random number is generated and the key data for every logical sector is generated. And the key data enciphered with the password is written in the storage 1. At the time of the writing of data data is enciphered with key data and it writes in the storage 1.

[0045] After reading the key data in which the storage 1 was enciphered at the time of reading of data it decrypts with a password and key data is obtained. And the data read from the storage is decrypted with this key data.

[0046] Thus even if it analyzes a cryptogram by enciphering data with the key data generated apart from the password the enciphered key data is only decoded. For this reason it is hard to analyze a password and key data. Thereby the

decipherment of the password in the analysis of a cryptogram can be prevented.  
[0047] A key which is different from a password per logical sector by changing key data to one password in order to encipher using the key data generated independently can be given. For this reason using a different key for every logical sector it can encipher and the confidentiality of data can be improved.  
[0048] Although the field L1 is established in the smaller one of the logic block address the field L1 may be stored in the greatest portion of a logic block address.

[0049] Drawing 7 is a writing processing flow chart of a 2nd embodiment of this invention. Drawing 7 explains the writing processing of a medium. Processing at the time of logical format creation of a medium is performed like the embodiment of drawing 2 and the key data in which each logical sector was enciphered by the storage 1 is stored.

[0050] (S30) Logic block-address (sector number) LBA presupposes that the write request to the position of "S0" arose. In order to keep the position which carries out a write request from lapping with the field L1 demanded sector number LBA is changed into "S1." Hereas shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0051] (S31) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc 1 and it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S34.

[0052] (S32) If the data of the field L1 reads CPU2 and it is not settled it will perform processing which develops key data to the work area of the memory 3. That is CPU2 obtains the user password PW. And data PS' of the field L1 of the optical disc 1 [1]-PS' [n] is read.

[0053] (S33) CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted with the password PW. Thereby it is key data PS. [1]-PS [n] is obtained. This key data PS [] (PS[1]-PS [n]) It stores in the work area of the memory 3.

[0054] (S34) CPU2 generates the random number R. And CPU2 is key data PS of logic block-address (sector number) LBA (=S0) of the key data of the work area of the memory 3. The random number R is written in [S0].

[0055] (S35) and CPU2 are this key data PS about the data which should be written in. [S0] It enciphers by (the random numbers R). Well-known DES etc. can be used as the method of encryption. CPU2 writes this enciphered data in the position of logic block-address LBA (=S1) of the optical disc 1.

[0056] (S36) CPU2 is suitable timing and it rewrites the data of the field L1 of the optical disc 1. That is when the value WC of the writing counter in which writing frequencies are shown exceeds 32 times for example in order that it may rewrite the field L1 for safety he follows CPU2 to Step S37. Even if the

situation where processing of medium discharge etc. is not made by a certain abnormalities arises it writes in for every fixed count in order to guarantee a certain amount of data restoration. The numerical value of 32 times is arbitrary. This processing is not the indispensable requirements for this invention. Since CPU2 saves key data when there is a discharge demand of the storage 1 he follows it to Step S37. Since CPU2 saves key data when OFF of a power supply arises he follows it to Step S37.

[0057] (S37) CPU2 is key data PS of a work area. [1]-PS Each of [n] is enciphered with the password PW. Of course key data PS of a work area [1]-PS The whole [n] may be enciphered with the password PW. Next key data PS' as which CPU2 was enciphered [1]-PS' [n] is written in the field L1 of the storage 1.

[0058] In addition to an operation of a 1st embodiment in the mode of the 2nd operation different key data is generated for every writing of data. For this reason it is enciphered by different key data for every writing of data and the privacy of data improves.

[0059] Since reading processing is the same as that of a 1st embodiment of drawing 6 explanation is omitted.

[0060] As for the writing processing flow chart of a 3rd embodiment of this invention and drawing 9 the explanatory view of the key data of a 3rd embodiment of this invention and drawing 10 of drawing 8 are the reading processing flow charts of a 3rd embodiment of this invention.

[0061] Key data PS' enciphered by the field L1 of the optical disc 1 like a 1st embodiment shown by drawing 2 at the time of the logical format of a medium [1]-PS' [512] is stored. However the enciphered key data is not stored for every logical sector here. For example the size of the field L1 shall be 4 KB. And when a password is 8 bytes / entry as shown in drawing 9 they are 512 keyword PS (entry). [1]-PS [512] is generated. And in the field L1 it is 512 keyword PS [which were enciphered]'. [1]-PS' [512] is stored.

[0062] Drawing 8 explains writing processing.

[0063] (S40) Logic block-address (sector number) LBA presupposes that the write request to the position of "S0" arose. In order to keep the position which carries out a write request from lapping with the field L1 demanded sector number LBA is changed into "S1." Hereas shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0064] (S41) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc 1 and it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S44.

[0065] (S42) If the data of the field L1 reads CPU2 and it is not settled it

will perform processing which develops key data to the work area of the memory 3. That is CPU2 obtains the user password PW. And data PS' of the field L1 of the optical disc 1 [1]-PS' [n] is read.

[0066] (S43) CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted with the password PW. Thereby it is key data PS. [1]-PS [n] is obtained. This key data PS [] (PS[1]-PS [n]) It stores in the work area of the memory 3.

[0067] (S44) CPU2 obtains the four values R0R1R2 and R3 from the demanded sector number S0. Here it considers that the logical sector number S0 is a 32-bit bit string and summarizes 8 bits at a time to the one value R0R1R2 and R3. R0-R3 become or more 0 less than 256 value. And R0-R3 are made into an index and it is PS of the work area of the memory 3. [] \*\* random number values (key data) are taken out. Based on four taken-out values 8 bytes of random number (key data) R is generated.

[0068] Key data PS corresponding to [ as here shown in drawing 9 ] R0 Key data PS corresponding to [ take out [R0] and ] (R1+256) [R1+256] is taken out. Key data PS corresponding to R2 Key data PS corresponding to [ take out [R2+256] and ] R3 [R3] is taken out.

[0069] And the key data R is calculated with the following computing equation.

[0070]

$$R = (PS[R0] * PS[R1+256] )$$

$$* (PS[R2+256] + PS[R3] )$$

\* is an EOR operation.

[0071] (S45) and CPU2 encipher the data which should be written in by this key data R. Well-known DES etc. can be used as the method of encryption. CPU2 writes this enciphered data in the position of logic block-address LBA (=S1) of the optical disc 1.

[0072] Next drawing 10 explains reading processing.

[0073] (S50) Logic block-address (sector number) LBA presupposes that the read request to the position of "S0" arose. In order to keep the position which carries out a read request from lapping with the field L1 demanded sector number LBA is changed into "S1." Here as shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0074] (S51) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc 1 and it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S54.

[0075] (S52) If the data of the field L1 reads CPU2 and it is not settled it will perform processing which develops key data to the work area of the memory 3. That is CPU2 obtains the user password PW. And data PS' of the field L1 of the optical disc 1 [1]-PS' [n] is read.

[0076] (S53) CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted with the password PW. Thereby it is key data PS. [1]-PS [n] is obtained. This key data PS [] (PS[1]-PS [n]) It stores in the work area of the memory 3.

[0077] (S54) CPU2 obtains the four values R0R1R2and R3 from the demanded sector number S0. It considers that the logical sector number S0 is a 32-bit bit stringand summarizes 8 bits at a time to the one value R0R1R2and R3. And R0-R3 are made into an indexand it is PS of the work area of the memory 3. [] \*\* random number values (key data) are taken out. Based on four taken-out values8 bytes of random number (key data) R is generated.

[0078] Key data PS corresponding to [ as here shown in drawing 9 ] R0 Key data PS corresponding to [ take out [R0] and ] (R1+256) [R1+256] is taken out. Key data PS corresponding to R2 Key data PS corresponding to [ take out [R2+256] and ] R3 [R3] is taken out.

[0079] And the key data R is calculated from the computing equation mentioned above.

[0080] (S55) and CPU2 read the data of logic block-address LBA (=S1) from the optical disc 1. The read data is decrypted by this key data R. Well-known DES etc. can be used as the method of decryption.

[0081] According to this 3rd embodimentit compares with a 1st embodiment and the size of the field L1 of the optical disc 1 can be made small. That isit is necessary to store the key data of the number of logical sectorsand the same number in a 1st embodiment. For examplewhen one sector shall be 2 KBa storage capacity shall be 600 MB and key data is set to 8Byteas for the field L1the capacity of 2.4 MB is needed. At a 3rd embodimentsince 512 key data is storedthe field L1 can be managed with about 4 KB.

[0082] And since a random number is generated by an operation even if it does in this waydifferent key data for every sector is obtained.

[0083] Drawing 11 is an explanatory view of a 4th embodiment of this inventionand drawing 12 is a writing processing flow chart of a 4th embodiment of this invention.

[0084] In addition to a 3rd embodimentthis 4th embodiment shows how to use two or more user passwords. As shown in drawing 11in order to accept a user to n namethe passwords PW1-PWn are set up for every user. Corresponding to each user8 bytes (size of PW1) of fields L2-Ln and 8 bytes of fields C1-Cn are established in the optical disc 1 noting that a password is 8 bytes.

[0085] When creating the logical format of a storagewhat enciphered random number data by user password PW1 is written in the field L1 like a 3rd embodiment.

[0086] Besidesin additioncharacter string DC1 for verification of a password is generatedand what enciphered this by password PW1 is written in the field C1. What enciphered password PW1 by PW2 is written in the field L2and what

enciphered password PW1 by PWn is written in the field Ln.

[0087] What enciphered character string DC2 for verification of password PW2 by password PW2 is written in the field C2. Hereafter what enciphered the character string DCn for verification of the password PWn with the password PWn is written in the field Cn.

[0088] The password which the character string for verification of each password entered verifies whether it is the right. This character string for verification is good also as a value (for example the password PWi exclusive OR with a certain specific character string) which may consist of secret character strings peculiar to a system and is calculated from the password PWi.

[0089] Next writing of the data in the case of using a user password and reading processing are performed like a 3rd embodiment shown in drawing 8 and drawing 10.

[0090] Drawing 12 explains the writing of the data in the case of using user password PWi (i>1).

[0091] (S60) Logic block-address (sector number) LBA presupposes that the write request to the position of "S0" arose. In order to keep the position which carries out a write request from lapping with the field L1 demanded sector number LBA is changed into "S1." Hereas shown in drawing 4 the sector number "S1" which applied the size "a" of the field L1 to the sector number "S0" and was changed is obtained.

[0092] (S61) CPU2 reads the data (enciphered key data) of the field L1 of the optical disc land it judges whether it is settled. Since it begins to read and key data is developed by the work area of the memory 3 if it is settled it progresses to Step S64.

[0093] (S62) If the data of the field L1 reads and it is not settled processing which develops key data to the work area of the memory 3 will be performed. That is CPU2 obtains the password PWi. And the field Li is read and the read data is decrypted with the password PWi. This obtains password PW1.

[0094] (S63) next CPU2 are data PS' of the field L1 of the optical disc 1. [1]-PS' [n] is read. CPU2 is data PS' of the field L1. [1]-PS' [n] is decrypted by password PW1. Thereby it is key data PS. [1]-PS [n] is obtained. This key data PS [] (PS[1]-PS [n]) It stores in the work area of the memory 3.

[0095] (S64) CPU2 obtains the four values R0R1R2 and R3 from the demanded sector number S0. Here it considers that the logical sector number S0 is a 32-bit bit string and summarizes 8 bits at a time to the one value R0R1R2 and R3. And R0-R3 are made into an index and it is PS of the work area of the memory 3. [] \*\* random number values (key data) are taken out. Based on four taken-out values 8 bytes of random number (key data) R is generated.

[0096] Key data PS corresponding to [ as here shown in drawing 9 ] R0 Key data PS corresponding to [ take out [R0] and ] (R1+256) [R1+256] is taken out. Key

data PS corresponding to R2 Key data PS corresponding to [ take out [R2+256] and ] R3 [R3] is taken out.

[0097] And the key data R is calculated with the computing equation mentioned above.

[0098] (S65) and CPU2 encipher the data which should be written in by this key data R. Well-known DES etc. can be used as the method of encryption. CPU2 writes this enciphered data in the position of logic block-address LBA (=S1) of the optical disc 1.

[0099] Thus two or more user passwords can be used.

[0100] Drawing 13 is a password change process flow figure (the 1) of a 4th embodiment of this invention and drawing 14 is a password change process flow figure (the 2) of a 4th embodiment of this invention.

[0101] In the composition of drawing 11 drawing 13 explains the processing which changes user password PW1.

[0102] (S70) CPU2 obtains old password PW1 and new password PW1'.

[0103] (S71) CPU2 reads the field L1 and the field C1 of the optical disc 1.

[0104] (S72) CPU2 decrypts the key data in which the field L1 was enciphered by password PW1 and it is key data PS. [ ] Obtain. And CPU2 decrypts the data of the field C1 by password PW1. The justification of password PW1 is judged from the decrypted character string for verification. If a password is not right it is considered as an error.

[0105] (S73) CPU2 is key data PS. [ ] Encipher by new password PW1' and write in the field L1 of the optical disc 1.

[0106] (S74) next CPU2 create character string DC1' for verification to new password PW1'. And CPU2 enciphers character string DC1' for verification by new password PW1' and it obtains write-in value C1'. CPU2 writes write-in value C1' in the field C1 of the optical disc 1.

[0107] Thus the justification of an old password can be checked and it can change into a new password. And change of a password can be performed without needing re-encryption of data. This method is an effective method when the number of user passwords is one.

[0108] When two or more user passwords are set up processing of drawing 13 is performed and when it changes into a new password a data access with the user passwords PW2-PWn becomes impossible. What is necessary is to use only user password PWi (i>1) as a user's password without using password PW1 as a user password if this is inconvenient when two or more user passwords are set up.

[0109] Drawing 14 explains the processing which changes this user password PWi (i>1).

[0110] (S80) CPU2 obtains the old password PWi and new password PWi'.

[0111] (S81) CPU2 reads the field Li and the field Ci of the optical disc 1.

[0112] (S82) CPU2 decrypts the data in which the field Li was enciphered with

the password PWi and it obtains password PW1. And CPU2 decrypts the data of the field Ci with the password PWi. The justification of the password PWi is judged from the decrypted character string for verification. If a password is not right it is considered as an error.

[0113] (S83) CPU2 enciphers by new password PWi' and it writes password PW1 in the field Li of the optical disc 1.

[0114] (S84) next CPU2 create character string DCi' for verification to new password PWi'. And CPU2 enciphers character string DCi' for verification by new password PWi' and it obtains write-in value Ci'. CPU2 writes write-in value Ci' in the field Ci of the optical disc 1.

[0115] Thus the justification of the old password PWi is checked and the password PWi can be changed. Change of a password is possible also for this example without needing re-encryption of data.

[0116] The following modification is possible for this invention other than the mode of above-mentioned operation.

[0117] (1) Although the magneto-optical disc explained the storage it is applicable to other storages such as an optical disc, a magnetic disk and an IC card.

[0118] (2) The thing of other forms can also use the computing equation which asks for the random number R.

[0119] As mentioned above although the embodiment of the invention explained various modification is possible within the limits of the main point of this invention and these are not eliminated from the range of this invention.

[0120]

[Effect of the Invention] According to this invention the following effect is done so as explained above.

[0121] (1) Encipher data as a password using the key data generated independently not using a password as a cryptographic key as it is. Even if it analyzes a cryptogram the enciphered key data is only decoded. For this reason it is hard to analyze a password and key data. Thereby the decipherment of the password in the analysis of a cryptogram can be prevented.

[0122] (2) A key which is different from a password in storage unit such as a sector by changing key data to one password in order to encipher using the key data generated independently can be given. For this reason using a different key for every logical sector it can encipher and the confidentiality of data can be improved.

[0123] (3) In order to encipher it as a password furthermore using the key data generated independently even if it changes a password re-encryption of data becomes unnecessary. For this reason even hundreds of megabytes of mass storage medium can realize change of a password easily.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram of the 1 embodiment of this invention.

[Drawing 2] It is a process flow figure at the time of the logical format of a 1st embodiment of this invention.

[Drawing 3] It is a writing processing flow chart of a 1st embodiment of this invention.

[Drawing 4] It is an explanatory view of the storage area of a 1st embodiment of this invention.

[Drawing 5] It is an explanatory view of the key data of a 1st embodiment of this invention.

[Drawing 6] It is a reading processing flow chart of a 1st embodiment of this invention.

[Drawing 7] It is a writing processing flow chart of a 2nd embodiment of this invention.

[Drawing 8] It is a writing processing flow chart of a 3rd embodiment of this invention.

[Drawing 9] It is an explanatory view of the key data of a 3rd embodiment of this invention.

[Drawing 10] It is a reading processing flow chart of a 3rd embodiment of this invention.

[Drawing 11] It is an explanatory view of a 4th embodiment of this invention.

[Drawing 12] It is a writing processing flow chart of a 4th embodiment of this invention.

[Drawing 13] It is a password change process flow figure (the 1) of a 4th embodiment of this invention.

[Drawing 14] It is a password change process flow figure (the 2) of a 4th embodiment of this invention.

[Drawing 15] It is an explanatory view of conventional technology.

[Description of Notations]

1 Optical disc (storage)

2 Control circuit (CPU)

3 Memory

20 The 1st encryption section

21 The 2nd encryption section

22 The 1st decoding section

23 The 2nd decoding section

---